jc534 U.S. PTO
09/24/99

a

PATENT

Docket No. IL-10360

jc534 U.S. PTO
09/405031
09/24/99

Assistant Commissioner for Patents
Washington, DC 20231

NEW APPLICATION TRANSMITTAL

Transmitted herewith for filing is the patent application of Inventor(s):
Douglas R. Coffland

For (title): **SYSTEM AND METHOD FOR MULTIMEDIA ENCRYPTION**

1. Type of Application

- ■ This new application is for an original patent.
- ❑ This new application is a:
  - ❑ Division
  - ❑ Continuation
  - ❑ Continuation-in-part (CIP)

2. Benefit of Prior U.S. Application(s) (35 USC 120)

- ❑ The new application being transmitted claims the benefit of prior U.S. application(s).

3. ❑ Benefit under 35 U.S.C. 119(e) of United States provisional application(s) listed below:

Application Serial No.	Filing Date

4. Papers enclosed which are required for filing Date Under 37 CFR 1.53(b).

- 13 Pages of specification
- 7 Pages of claims
- 1 Pages of abstract
- 5 Sheets of drawings
  - ■ formal
  - ❑ informal

5. Additional papers enclosed

- ❑ Preliminary Amendment
- ■ Information Disclosure Statement
- ■ Form PTO-1449
- ❑ Special Comments

6. **Declaration or oath**

- ■ Enclosed and executed by
  - ■ inventors
  - ❑ legal representative of inventor(s) 37 CFR 1.42 or 1.43
- ❑ Not Enclosed

7. **Assignment**

- ■ An assignment of the invention to The Regents of the University of California.
  - ■ is attached
  - ❑ will follow

8. **Certified Copy**

Certified copy(ies) of application(s)

(country)	(application no.)	(filed)
(country)	(application no.)	(filed)

from which priority is claimed

- ❑ is(are) attached.
- ❑ will follow

9. **Fee Calculation**

CLAIMS AS FILED

Type of Claim	Number Filed	Included in Basic Fee	Number Extra	Rate	Total Fee
Total Claims	30	-20 =	10	x $18 =	$ 180.00
Independent Claims	4	-3 =	1	x $78 =	$ 78.00
				Multiple Claims =	$
				Basic Filing Fee =	$ 760.00
				Sub-Total =	$ 1,018.00
				Small Entity Filing Fee =	**$ 509.00**

10. Small Entity Statement(s)

■ Verified Statement that this is a filing by small entity under 37 CFR 1.9 and 1.27 is attached.

Filing Fee Calculation (50% of regular filing fee) $ 509.00

11. Fee Payment

❑ Not Enclosed

■ Enclosed (See Account No. Below)

Total Basic Filing Fees To Be Paid **$ 509.00**

12. Method of Payment of Fees

❑ Check in the Amount of $ _____

■ Charge Account No. **12-0695** in the amount of $ **509.00**

A duplicate of this transmittal is attached.

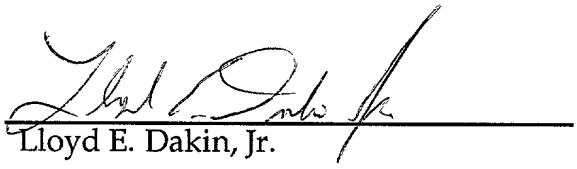
13. Instructions As To Overpayment/Underpayment

■ credit/charge
Account No. **12-0695**

❑ refund

Reg. No.: 38,423

Tel. No.: (925) 423-8554



Lloyd E. Dakin, Jr.
P.O. Box 808, L-703
Livermore, CA 94551

Dated: September 1, 1999

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Douglas R. Coffland

Attorney Docket No. : IL-10366

Serial No. :

Art Unit:

Filed :

Examiner:

For : System and Method for Multimedia Encryption

jc#94 U.S. PTO
09/405031
09/24/99

Assistant Commissioner for Patents
Washington, D.C. 20231

EXPRESS MAIL CERTIFICATE

"Express Mail" label number EL269945990US

Date of Deposit September 24, 1999

I hereby certify that the following *attached*

1. Recordation Cover Sheet
2. Assignment (1 page)
3. New Application Transmittal (in duplicate)
4. Combined Declaration and Power of Attorney (2 pages)
5. Verified Statement Claiming Small Entity Status
6. Application
   (Specification 13 pages, Claims 7 pages, Abstract 1 page)
   Five (5) sheets of formal drawings;
7. Information Disclosure Statement, Form 1449,
   1 copy each of 5 patents and 1 publication
8. Return postcard

is being deposited with the United States Postal Service "Express Mail Post Office to addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Box: Patent Application, Washington, D.C. 20231.

Nancy J. Stone
(Type or print name of person mailing paper)

Nancy J. Stone
(Signature of person mailing paper or fee)

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant :	Douglas R. Coffland	Docket No. :	IL-10360
Serial No. :		Art Unit :	
Filed :		Batch No. :	
For :	System and Method for Multimedia Encryption	Examiner :	

VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS [37 CFR 1.9 (f) and 1.27(d)] - NONPROFIT ORGANIZATION

I hereby declare that I am an official empowered to act on behalf of the nonprofit organization identified below:

The Regents of the University of California
1111 Franklin Street
Oakland, CA 94607-5200

TYPE OF ORGANIZATION

__X__University or Other Institution of Higher Education

I hereby declare that the nonprofit organization identified above qualifies as a nonprofit organization as defined in 37 CFR 1.9(e) for purposes of paying reduced fees under Section 41(a) and (b) of Title 35, United States Code with regard to the invention entitled System and Method for Multimedia Encryption

by inventor(s) Douglas R. Coffland

described in

_X_ the specification filed herewith.

___ application serial no. _____, filed _____.

___ patent no. _____, issued _____.

I hereby declare that rights under contract or law have been conveyed to and remain with the nonprofit organization with regard to the above identified invention, except for a license to a Federal Agency pursuant to 35 USC 202(c) (4).

Each person, concern or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey, or license any rights in the invention is listed below:

_X_ no such person, concern, or organization

I acknowledge the duty to file, in this application or patent, notification of any charge in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true: and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

JANET G. TULK
Laboratory Counsel
Lawrence Livermore National Laboratory
7000 East Avenue, L-701
Livermore, CA 94551

Janet G. Tulk
JANET G. TULK

Sept 1, 1999
Date

S- 91,131

IL-10,360

SYSTEM AND METHOD FOR MULTIMEDIA ENCRYPTION

BY

Douglas R. Coffland (USA)
5674 Wisteria Way
Livermore, CA 94550

SYSTEM AND METHOD FOR MULTIMEDIA ENCRYPTION

The United States Government has rights in this invention pursuant to Contract No. W-7405-ENG-48 between the United States Department of Energy and the University of California for the operation of Lawrence Livermore National Laboratory.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to systems and methods for encryption, and more particularly for multimedia encryption.

2. Discussion of Background Art

Transmission of audio and video signals, such as video conferencing and security surveillance signal, across both local and wide area networks is becoming more and more commonplace in today's globally interconnected internet driven economy. In such applications, encryption is often required for protecting and authenticating such multimedia signals as they travel over unsecured networks. For instance, corporations often exchange business sensitive information during such conferences which must not be intercepted. Additionally, multimedia information from networked security camera systems must be authenticated and protected from unauthorized monitoring.

A degree to which encryption authenticates and protects multimedia data depends on the encryption schema used, an encryption key length, the predictability of the encryption key, and how the encryption keys are protected. Typically, encryption keys are generated by hashing algorithms from random number seeds provided by a source which hopefully provides random number seeds. Random number seeds, however, are extremely difficult if not impossible to generate using algorithmic methods on digital computers, since algorithms executing on digital computers are by nature deterministic. As a result, various external chaotic sources have been used to generate the random number seeds.

Examples include methods described in U.S. Patent 5,732,138 entitled, "Method For Seeding A Pseudorandom Number Generator With A Cryptographic Hash Of A Digitization Of A Chaotic System," by Noll et al., and U.S. Patent 5,774, 549 entitled, "Method And Apparatus That Processes A Video Signal To Generate A Random Number Generator Seed" by Jakob Nielsen.

Noll discusses generating seeds by applying a hashing algorithm to a digitized chaotic system. Chaotic systems mentioned include clouds moving in the sky, ocean waves crashing on a shoreline, and nodules moving within a "lava-lamp." A weakness of the Noll system, however, is that in his preferred embodiment, new seed generation depends upon using dedicated input devices to monitor "real-world scenes," such as a video camera

monitoring a lava-lamp, in order to obtain the necessary chaotic input for eventual random number generation.

Nielsen also requires dedicated input devices, such as a video camera. Nielsen monitors "live" scenes with a video camera and then generates seeds from pixel changes within sequential frames of video data. A weakness of the Nielsen system is that new seeds are not generated when motion within a monitored scene stops.

In response to the concerns discussed above, what is needed is a system and method for multimedia encryption that overcomes the problems of the prior art.

SUMMARY OF THE INVENTION

The present invention is a system and method for multimedia encryption. Within the system of the present invention, a data compression module receives and compresses a media signal into a compressed data stream. A data acquisition module receives and selects a set of data from the compressed data stream. And, a hashing module receives and hashes the set of data into a keyword.

In other aspects of the invention, the system may include a data compression module that compresses the media signal into any compression format that has varying length data frames. Examples of media compression formats that with varying length data frames include MPEG1, MPEG2, MPEG4, MJPEG, and H.261. The set of data can be one frame of data, cross over several frame boundaries, include compression transform coefficients, include predictive data frames. Finally, a pseudo-random number generator can processes a single keyword seed in to a set of keywords.

The method of the present invention includes the steps of compressing a media signal into a compressed data stream; selecting a set of data from the compressed data stream; and hashing the set of data into a keyword.

The system/apparatus and method of the present invention are particularly advantageous over the prior art because a means of capturing random numbers for encryption seeding directly from variable frame boundary compressed data is disclosed. In light of a growing importance in

securely transmitting multimedia data over digital networks, obtaining random numbers directly from the multimedia data would be very useful.

These and other aspects of the invention will be recognized by those skilled in the art upon review of the detailed description, drawings, and claims set forth below.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of a system for multimedia encryption according to the present invention;

Figure 2 is a graphical depiction of quantization processes within an analog-to-digital converter within the system;

Figure 3 is a block diagram of a computer within the system;

Figure 4 is a graphical depiction of how a data acquisition module operates within the system; and

Figure 5 is a flowchart of a method for multimedia encryption.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Figure 1 is a block diagram of a system 100 for multimedia encryption according to the present invention. Within the system 100, a transducer 102, such as a video camera, a radio, a microphone, a Geiger counter, or an electrical component, outputs a media signal 104.

The media signal 104 may or may not contain useful information, such as an actual video scene or audio output, and the present invention does not require that useful information be present. For example, while a video camera could be capturing a scene, this is not required, and instead a lens-cap could be on the camera causing the scene to be perfectly quiescent. In one embodiment of the present invention, the media signal need only include random transducer noise having a noise signal amplitude. Random noise is not the same a chaotic noise. Random noise, such as white Gaussian noise, is completely unpredictable from one moment to a next, while chaotic noise is highly predictable over short time periods. In a second embodiment of the invention, however, random transducer noise need not even be present. Instead, data compression techniques provide a basis for multimedia encryption, as will be elaborated upon below.

The media signal 104 from the transducer 102 is fed into an analog-to-digital (A/D) converter 106. The converter 106 quantizes the media signal with a quantization step size smaller than the noise signal amplitude within the media signal 104, creating a quantized media signal 108. The quantized media signal 108 is then routed to a computer 110.

Figure 2 is a graphical depiction of quantization processes within the analog-to-digital converter 106 within the system 100. The media signal 104 is periodically sampled 202. The samples 202 are then quantized at predefined steps 204 resulting in the quantized media signal 108. The quantized media signal 108 is a quantized approximation of the media signal 104 containing random transducer noise. The random noise in the media signal 104 will cause even unchanging video scenes to have quantization values 206 which fluctuate for media signal values close to one or more quantization steps 204. Thus, even a perfectly quiescent media signal 104 (e.g. when a lens cap is on a video camera containing the transducer 102) will contain some randomness from random transducer noise. Put another way, as long as a size of a smallest quantizer step is no larger than an amplitude of the transducer 102 noise, the quantized media signal 108 will include a high level of randomness even if input to the transducer is perfectly quiescent.

Typically, the transducer noise is sufficient to cause the quantization values 206 to fluctuate. However, if the transducer noise is small relative to the quantization steps 204, then either video or audio content of the media signal 104 must vary somewhat so that what little noise is in the scene will enable random noise to be quantized by the A/D converter 106. Randomness will be present in the media signal 104 when an actual sampled media signal value 208 is very close to a quantization boundary 210. When this occurs, a small transducer 102 signal will randomly cause the quantized media signal

108 to vary. It is possible to test whether sufficient random noise is present within the media signal 104 by looking at least significant bits of the media signal 104 and ensuring that no long sequences of a single bit value (i.e. ones or zeros) exist. Long sequences of zeros or ones in a least significant bit of the media signal 104 would suggest that the random noise is not of a sufficient amplitude to create random numbers.

In an alternate embodiment, distortion may be introduced into the media signal 104 generated by the transducer 102 such that the random transducer noise will have an amplitude greater than the quantization steps 204. Distortion may be introduced, for example, in a video camera by turning on an automatic gain control and increasing video camera gain. In another embodiment, focus and zoom of the camera can be varied while capturing video data.

Figure 3 is a block diagram 300 of the computer 110 within the system 100. Within the computer 110, a data compression module 302 compresses the quantized media signal 108 into a compressed data stream 303 using any number of formats, such as MJPEG, MPEG1, MPEG2, MPEG4, or H.261. Many other standard, as well as proprietary, media compression schemes also exist that are compatible with the present invention.

The compressed data stream 303 is partitioned into data frames of varying length, depending upon an amount of information contained in the media signal 104, variations in a scene or audio captured by the transducer

102, transducer noise, and system noise. For example, a 16384 byte amount of data acquired from an MPEG1 compressed data stream can include between one and eight frames of media data of varied length. For comparison, uncompressed media signals generally have a frame length which is fixed in size. For instance, uncompressed digital video signals include a series of fixed sized digital video images.

Under some compression schemas, the compressed data stream 303 includes predictive data frames. Predictive data frames only contain information which reports on differences between a current data frame and a most recent full data frame. Predictive data frames typically include motion vectors and error codes. Identical motion vectors and error codes between full frames indicate an absence of any video motion, audio, or transducer noise.

The compressed data stream 303 also can include compression transform coefficients, frame sequence numbers, and cyclic redundancy checks which vary from frame to frame. Identical transform coefficients between full frames indicate an absence of any video motion, audio, or transducer noise.

In response to a key request 304 received from an external source (not shown), a control module 306 instructs a data acquisition module 308 to collect a set of data 309 from the compressed data stream 303. The data acquisition module 308 operating in conjunction with the data compression module 302 creates a robust source of random numbers in the set of data 309.

This is due to unpredictable variability between the compressed data stream 303 and random selection of the set of data 309 therefrom.

In an alternate embodiment, the data acquisition module 308 can be instructed to collect the set of data 309 directly from the quantized media signal 108 output by the A/D converter 106 before any data compression. An amount of data collected is dependent upon an amount of uncertainty required for a given application. A good rule of thumb is to capture an amount of data greater than or equal to a compressed full frame. However, when a large amount of noise is present in the media signal, a lesser amount of the media signal data needs to be collected.

A message digest generator 310 receives and processes the set of data 309 with a hashing algorithm. The message digest generator 310 generates a fixed-length unique identifier 311 for each pattern of bits in the set of data 309. Hashing algorithms assure that the resultant identifier 311 varies significantly even if the set of data 309 only varies by one bit. It is computationally infeasible to reconstruct the set of data 309 from only knowledge of the identifier 311. This identifier 311 is also called a keyword seed.

An encryption key generator 312 is a pseudo-random number generator that receives and processes the identifier 311 into a set of keywords to be immediately used or stored in a memory 314 for later use.

Figure 4 is a graphical depiction 400 of how the data acquisition module 308 operates within the system 100. Shown is a typical compressed

multimedia data stream 402. The data stream 402 includes compressed audio, video, and control data separated by frame boundaries 404. Each frame of data has a length, such as video data 406, which has a length 408. Within the multimedia data stream, lengths of each frame vary randomly, depending on a compression ratio as well as other well known compression algorithm factors. The data acquisition module 308 acquires a set of data 410 from the compressed data stream 303 without regard to any of these factors.

Thus, the set of data 410 can cross over the frame boundaries 404 in a random manner, resulting in a highly random, and unpredictable set of data 309. The set of data 309 thus can function as a robust keyword seed.

Figure 5 is a flowchart 500 of a method for multimedia encryption. The method begins in step 502 where the transducer 102 receives a media signal which may include a noise signal amplitude. In step 504, the A/D converter 106 quantizes the media signal with a quantization step size smaller than the noise signal amplitude. The data compression module 302 compress the media signal into data frames having data frame boundaries, where the data frames may have similar or varying lengths, include compression transform coefficients, and/or include predictive data frames in step 506. Next, in step 508, the data acquisition module 308 selects a set of data from the compressed media signal, such that the data selected may include one frame of data, data which crosses over several data frame boundaries, compression transform coefficients, and/or predictive data frames. In step 510, the message digest

generator 310 hashes the set of data into a keyword. After step 510, the method is complete.

While the present invention has been described with reference to a preferred embodiment, those skilled in the art will recognize that various modifications may be made. Variations upon and modifications to the preferred embodiment are provided by the present invention, which is limited only by the following claims.

WHAT IS CLAIMED IS:

1. A system for multimedia encryption comprising:

a media signal;

a data compression module coupled to receive and compress the media signal into a compressed data stream;

a data acquisition module coupled to receive and select a set of data from the compressed data stream; and

a hashing module coupled to receive and hash the set of data into a keyword.

2. The system of claim 1 wherein the set of data is one frame of data within the compressed data stream.

3. The system of claim 1 wherein the set of data crosses over several frame boundaries within the compressed data stream.

4. The system of claim 1 wherein:

the compressed data stream includes compression transform coefficients; and

the set of data includes a set of compression transform coefficients.

5. The system of claim 1 wherein:

the compressed data stream includes data frames of varying length; and

the set of data includes a set of data frames.

6. The system of claim 1 wherein:

the compressed data stream includes predictive data frames; and

the set of data includes a predictive data frame.

7. The system of claim 1:

wherein the media signal includes a noise signal amplitude;

further comprising,

an analog to digital converter, having a quantization step size smaller than the noise signal amplitude, coupled to receive and quantize the media signal; and

wherein the data compression module compresses the quantized media signal into a compressed data stream.

8. The system of claim 1 wherein the data compression module compresses the media signal into one from a group consisting of: MJPEG, MPEG1, MPEG2, or MPEG4, H.261, H.320, and H.323 formats.

9. The system of claim 1 further comprising:

a pseudo-random number generator coupled to receive and process the keyword in to a set of keywords.

10. A method for multimedia encryption, comprising the steps of:

compressing a media signal;

selecting a set of data from the compressed media signal; and

hashing the set of data into a keyword.

11. The method of claim 10 wherein:

the compressed media signal includes data frames; and

the selecting step includes the step of selecting one frame of data.

12. The method of claim 10 wherein:

the compressed media signal includes data frames and data frame boundaries; and

the selecting step includes the step of selecting a set of data which crosses over several data frame boundaries.

13. The method of claim 10 wherein:

the compressed media signal includes compression transform coefficients; and

the selecting step includes the step of selecting a set of compression transform coefficients.

14. The method of claim 10 wherein:

the compressed media signal includes data frames of varying length; and

the selecting step includes the step of selecting a set of data frames.

15. The method of claim 10 wherein:

the compressed media signal includes predictive data frames; and

the selecting step includes the step of selecting a predictive data frame.

16. The method of claim 10:

wherein the media signal includes a noise signal amplitude;

further comprising the step of quantizing the media signal with a quantization step size smaller than the noise signal amplitude; and

wherein the compressing step includes the step of compressing the quantized media signal.

17. A system for multimedia encryption, comprising:

means for compressing a media signal;

means for selecting a set of data from the compressed media signal; and

means for hashing the set of data into a keyword.

18. The system of claim 17 wherein:

the compressed media signal includes data frames; and

the means for selecting includes means for selecting one frame of data.

19. The system of claim 17 wherein:

the compressed media signal includes data frames and data frame boundaries; and

the means for selecting includes means for selecting a set of data which crosses over several data frame boundaries.

20. The system of claim 17 wherein:

the compressed media signal includes compression transform coefficients; and

the means for selecting includes means for selecting a set of compression transform coefficients.

21. The system of claim 17 wherein:

the compressed media signal includes data frames of varying length; and

the means for selecting includes means for selecting a set of data frames.

22. The system of claim 17 wherein:

the compressed media signal includes predictive data frames; and

the means for selecting includes means for selecting a predictive data frame.

23. The system of claim 17:

wherein the media signal includes a noise signal amplitude;

further comprising means for quantizing the media signal with a quantization step size smaller than the noise signal amplitude; and

wherein the means for compressing includes means for compressing the quantized media signal.

24. A computer-useable medium embodying computer program code for multimedia encryption by executing the steps of:

compressing a media signal;

selecting a set of data from the compressed media signal; and

hashing the set of data into a keyword.

25. The computer-useable medium of claim 24 wherein:

the compressed media signal includes data frames; and

the selecting step includes the step of selecting one frame of data.

26. The computer-useable medium of claim 24 wherein:

the compressed media signal includes data frames and data frame boundaries; and

the selecting step includes the step of selecting a set of data which crosses over several data frame boundaries.

27. The computer-useable medium of claim 24 wherein:

the compressed media signal includes compression transform coefficients; and

the selecting step includes the step of selecting a set of compression transform coefficients.

28. The computer-useable medium of claim 24 wherein:

the compressed media signal includes data frames of varying length; and

the selecting step includes the step of selecting a set of data frames.

29. The computer-useable medium of claim 24 wherein:

the compressed media signal includes predictive data frames; and

the selecting step includes the step of selecting a predictive data frame.

30. The computer-useable medium of claim 24:

wherein the media signal includes a noise signal amplitude;

further comprising the step of quantizing the media signal with a quantization step size smaller than the noise signal amplitude; and

wherein the compressing step includes the step of compressing the quantized media signal.

SYSTEM AND METHOD FOR MULTIMEDIA ENCRYPTION

ABSTRACT OF THE DISCLOSURE

A system and method is disclosed for multimedia encryption. Within the system of the present invention, a data compression module receives and compresses a media signal into a compressed data stream. A data acquisition module receives and selects a set of data from the compressed data stream. And, a hashing module receives and hashes the set of data into a keyword. The method of the present invention includes the steps of compressing a media signal into a compressed data stream; selecting a set of data from the compressed data stream; and hashing the set of data into a keyword.

SUBSTITUTE SHEET (RULE 26)

100

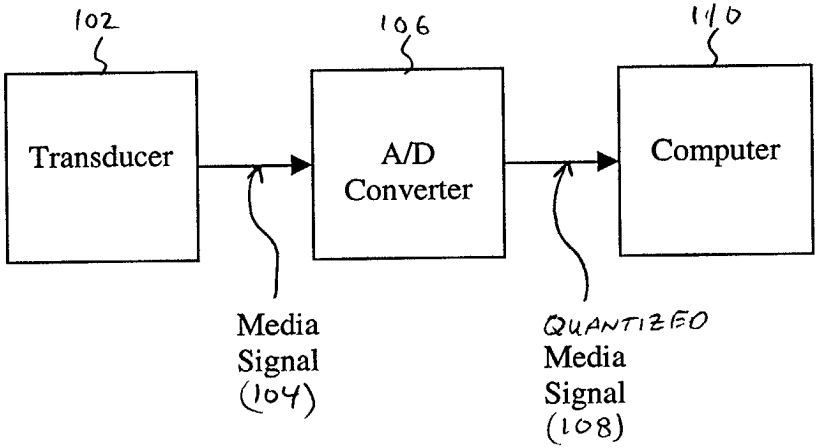


FIG. 1

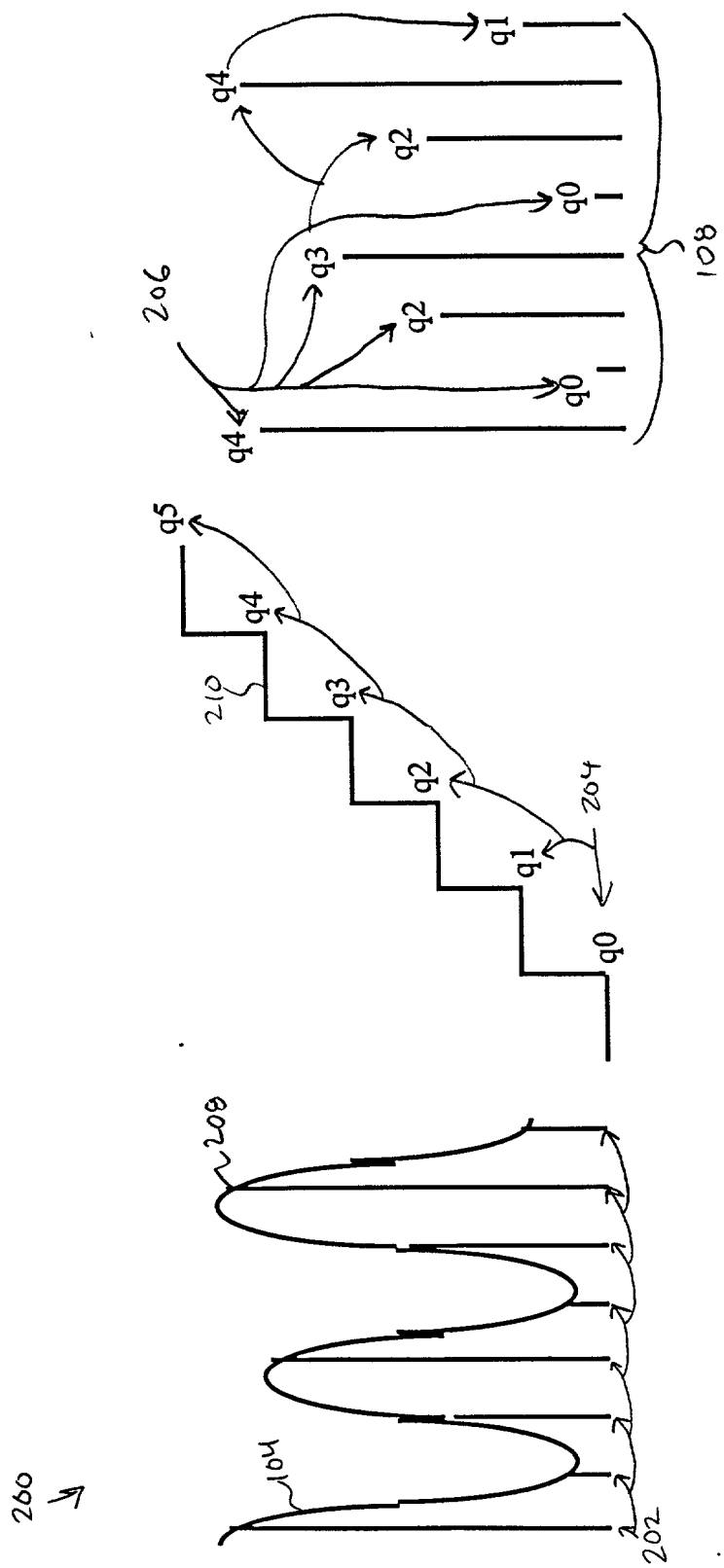

200
104
208
202
q5
q4
q3
q2
q1
q0
210
204
206
q4
q0
q3
q2
q0
q4
q2
q1
108

FIG. 2

SUBSTITUTE SHEET (RULE 26)

300

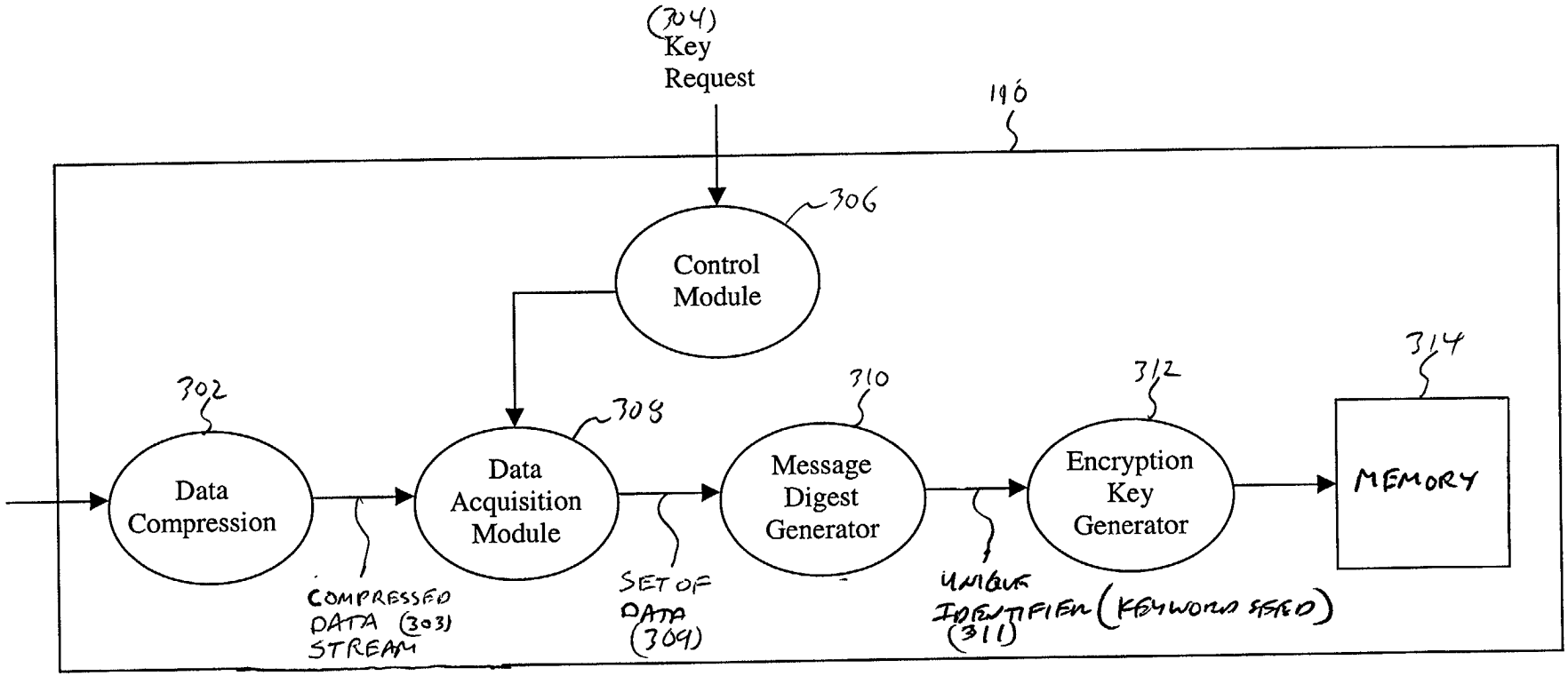


FIG. 3

SENSO TECHNO

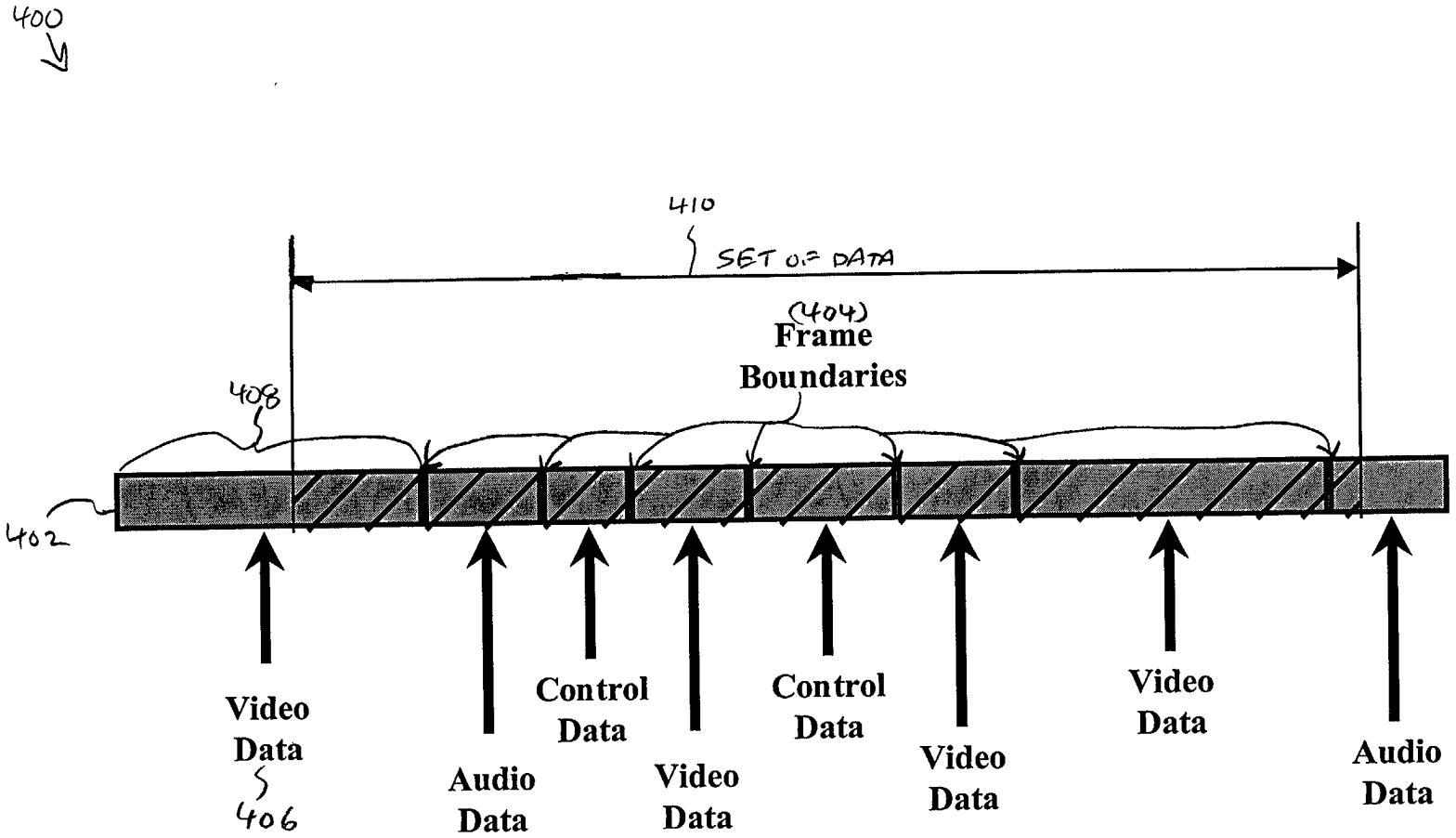


FIG. 4

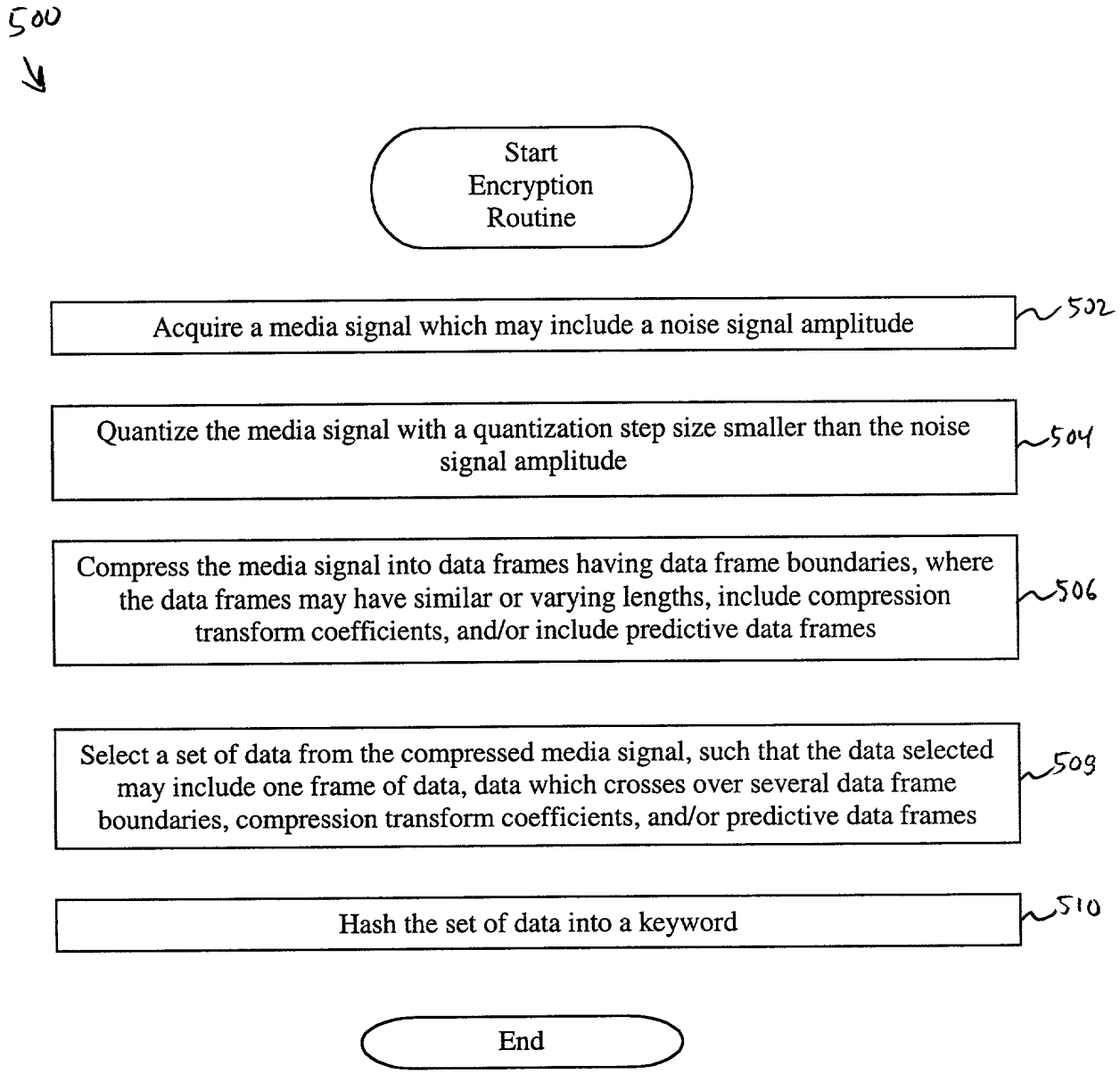

500
Start Encryption Routine
Acquire a media signal which may include a noise signal amplitude
502
Quantize the media signal with a quantization step size smaller than the noise signal amplitude
504
Compress the media signal into data frames having data frame boundaries, where the data frames may have similar or varying lengths, include compression transform coefficients, and/or include predictive data frames
506
Select a set of data from the compressed media signal, such that the data selected may include one frame of data, data which crosses over several data frame boundaries, compression transform coefficients, and/or predictive data frames
508
Hash the set of data into a keyword
510
End

FIG. 5

COMBINED DECLARATION AND POWER OF ATTORNEY

■ Declaration submitted with Initial Filing
❑ Declaration submitted after Initial Filing (surcharge (37 CFR 1.16(e)) required)

Attorney Docket: IL-10360
Applicant: Douglas R. Coffland
Serial No.:
Filing Date:

As a below named inventor(s), I (we) hereby declare that:

My (Our) residence, post office address and citizenship(s) are as stated below next to my (our) name(s).

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: _____
System and Method for Multimedia Encryption

the specification of which (check one)

_X_ is attached hereto ____was filed on _____ as United States Application Number

or PCT International Application Number _____

and was amended on _____(if applicable).

I (We) hereby state that I (we) have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I (We) acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56.

I (We) hereby claim foreign priority benefits under 35, U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)			Priority Not Claimed
(Application Number)	(Country)	(Foreign Filing Date)	❑
(Application Number)	(Country)	(Foreign Filing Date)	❑

I (We) hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below:

Application Serial No.	Filing Date
Application Serial No.	Filing Date

I (We) hereby claim the benefit under 35 U.S.C. 120 of any United States applications(s), or 365(c) of any PCT international application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

Application Serial No.	Filing Date	Status

POWER OF ATTORNEY: As the named inventor(s), I (we) hereby appoint the following registered practitioner(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Names	Registration No.
Lloyd E. Dakin, Jr.	38,423
John P. Wooldridge	38,725

Direct Correspondence To:	Direct Telephone Calls To: (Name and Telephone Numbers)
Lloyd E. Dakin, Jr. Assistant Laboratory Counsel Lawrence Livermore National Laboratory P.O. Box 808 - L-703 Livermore, California 94551	Lloyd E. Dakin, Jr. (925) 423-8554

I (We) hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Douglas R. Coffland	Douglas R Coffland
Full Name of Inventor	Signature
Livermore, California	9/10/99
Residence (City, State or Foreign Country)	Date
5674 Wisteria Way, Livermore, CA 94550	USA
Postal Address (Street, City, State, Zip Code)	Citizenship
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	
Full Name of Inventor	Signature
Residence (City, State or Foreign Country)	Date
Postal Address (Street, City, State, Zip Code)	Citizenship
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	